УДК 661.3.066

**А. В. Шабров, А. В. Гаврыш**
Научный руководитель: аспирант К. Л. Стойчин
Уральский федеральный университет, Екатеринбург

# ПРОБЛЕМА НАЛИЧИЯ УЯЗВИМОСТЕЙ ИНФОКОММУНИКАЦИОННОЙ СТРУКТУРЫ ПРЕДПРИЯТИЯ И ПУТИ ЕЕ РЕШЕНИЯ

*Аннотация.* В статье рассмотрены актуальные вопросы уязивимостей инфокоммуникационной структуры современных предпиятий, а также проведене анализ нарушителей и угроз.

*Ключевые слова:* предприятие; хищение; инфокоммуникационная структура; информационная структура; USB-ключ; защита информации; видеонаблюдение.

В условиях современного рынка существование множества предприятий обусловлено тем, что они осуществляют деятельность, результатом которой является коммерческая тайна в различных ее видах. Это может быть продукт, технология или изделие. Также коммерческая тайна может содержаться в контактных данных поставщиков, потребителей, клиентов, информационных, производственно-технологических новшествах и полезных изобретениях. Благодаря строгому и точному соблюдению мер по защите информации такого рода, предприятия могут существовать и иметь высокую динамику развития. Но существует неограниченное количество методов, средств и технологий, направленных на хищение информации такого рода. Подавляющее большинство сведений конфиденциального характера коммерческих предприятий хранится и обрабатывается в информационной системе предприятия, средой передачи данных для которой является инфокоммуникационная структура. Темой данной статьи является анализ уязвимостей инфокоммуникационной структуры предприятия. Актуальность данной статьи заключается в том, что любая инфокоммуникационная структура имеет уязвимости, которые необходимо учитывать при построении стратегии информационной безопасности предприятия.

Инфокоммуникационная структура — это технологическая система, которая включает, кроме сети, связи также средства хранения, обработки и поиска информации. Она предназначена для обеспечения пользователей связью и доступом к необходимой информации. Под нарушением информационной безопасности предприятия следует понимать комплекс противоправных действий, направленных на несанкционированный доступ, получение и распро-

© А. В. Шабров, А. В. Гаврыш, 2017

странение информации, осуществляемых как с использованием средств вычислительной техники, программного обеспечения и коммуникаций, так и без них. При реализации угроз безопасности информационные и коммуникационные технологии могут выступать в качестве объекта преступления, средства преступления, средства подготовки преступления или среды совершения преступления. Реализация нарушителями угроз безопасности инфокоммуникационной структуры предприятия приводит к нарушению нормального функционирования или к снижению безопасности информации, определенное конфиденциальностью, целостностью и доступностью. Обеспечение информационной безопасности сводится к трем основным направлениям — это комбинация технических, административных и организационных мер. Прежде всего нужно понять, что и от чего необходимо защитить. Как правило, предприятия в процессе реализации ИБ применяют такие малоэффективные меры, как, например, блокировку интернет-пейджеров или фильтр электронной почты, глушилки сотовой связи. Однако всегда найдутся альтернативные каналы. Однозначно из этого следует вывод, что защита от утечек должна быть всеобъемлющей, охватывающей все процессы предприятия. Исходя из вышеизложенного, необходимо разрабатывать соответствующие методы и средства обеспечения информационной безопасности информационных систем, среди них можно предложить следующие: совершенствование системы аутентификации пользователей, защита информации внутри фирмы (при пересылке и хранении), разработка эффективной системы защиты от внутренних угроз, совершенствование системы аутентификации пользователей. Аутентификация (или идентификация) пользователя выполняется каждый раз, когда пользователь вводит логин и пароль для доступа к компьютеру, в Сеть или при запуске прикладной программы. В результате их выполнения он получает либо доступ к ресурсу, либо отказ в доступе. Оптимальное решение проблемы — специальное программное обеспечение, позволяющее хранить пароли в защищенной памяти электронных идентификаторов и в нужный момент извлекать их и предоставлять соответствующим системным или прикладным компонентам. В качестве электронных идентификаторов могут использоваться USB-носители или смарт-карты, что позволяет контролировать их обращение и организовать строгий учет. Такие меры существенно снижают риск утечки информации, связанные с ошибками персонала, а также с преднамеренными действиями сотрудников, имеющих преступный умысел, и обеспечивают надежную аутентификацию пользователей при доступе к сетевым ресурсам.

Поскольку информация в корпоративных сетях хранится на носителях, и попадание именно этих носителей в руки злоумышленника создает наиболее серьезную угрозу информационной безопасности и может привести к тяжелым последствиям, оптимальным решением проблемы именно для защиты

информации в процессе хранения будет необходимость в защите информации, размещенной на носителях информации, методом шифрования данных на серверах, а также шифрование данных на дисках персональных компьютеров. Особое значение приобретает защита информации при резервном копировании. Разработка эффективной системы защиты от внутренних угроз. Обычный сотрудник компании, имеющий легальный доступ к сетевым и информационным ресурсам и обладающий определенными знаниями о структуре корпоративной сети, может нанести своей компании гораздо больший ущерб, чем внешний нарушитель, пытающийся как-либо получить доступ к информации из вне. Как правило, более 60 % попыток нарушения информационной безопасности предприятия происходит от внутреннего нарушителя.

Актуальная проблемой является то, что любой сотрудник предприятия может практически незаметно пронести на территорию предприятия компактный носитель любого объема и скопировать на него всю интересующую его информацию. Такая проблема решается простой и в то же время действенной мерой — это системы, блокирующие порты компьютера, к которым могут подключаться внешние устройства, и возможность гибкой настройки прав доступа на основе списков контроля доступа. Такие системы запрещают использование внешних накопителей информации и разрешают подключение только зарегистрированных внешних устройств, например, USB-ключей для аутентификации пользователей. Также присутствует возможность записи в журнал неудачных попыток подключения, которая, в свою очередь, позволит выявить потенциального нарушителя среди сотрудников. Перечисленные методы и средства, предотвращающие нарушения информационной безопасности, не являются совершенными и могут в дальнейшем совершенствоваться, хотя даже эти относительно простые способы защиты позволят существенно снизить риск несанкционированного доступа к информации.

Поскольку проблема обеспечения ИБ предприятия многогранна и дать универсальный совет на все случаи жизни достаточно проблематично, на начальном этапе нужно предпринять для снижения рисков нарушения информационной безопасности, проверку персонала при приеме на работу совместно с отделом безопасности и отделом по управлению персоналом. Как правило, это привычное всем тестирование, собеседование, определение личностных характеристик и наклонностей, но также и проверка предыдущих мест работ, так называемое наведение справок по всем возможным источникам информации. Это поможет отсеять потенциальных нарушителей еще до тех пор, как они устроятся на предприятие. Следующим этапом будет грамотная пользовательская политика внутри корпоративной сети. Разграничение прав и уровня доступа к отдельным видам информации, особенно к той, которая представляет коммерческую тайну. Следующий этап — постоянный контроль. Необходимо

применять различные средства мониторинга сетевого трафика, анализа сетевой активности, кто и что посещает в Сети и куда уходят письма с корпоративного ящика. Камеры видеонаблюдения и фиксация телефонных звонков также являются неотъемлемой частью защиты предприятия.

В ходе статьи было выяснено, что защита информации — есть комплекс мероприятий, проводимых владельцем информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям. А понятие информационной безопасности предприятия — это защищенность информации и поддержание инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба предприятию.

В итоге можно сделать вывод, что правильное, а самое главное — грамотное применение защиты информации на предприятии должно быть всеобъемлющее и должно охватывать все слабые стороны инфокоммуникационной структуры предприятия.

УДК 004.02

**С. В. Глухарева**
Научный руководитель: д-р тех. наук, проф. А. А. Шелупанов
Томский государственный университет систем управления
и радиоэлектроники, Томск

## МЕТОДИКА ПОДБОРА ПЕРСОНАЛА НА ДОЛЖНОСТИ, СВЯЗАННЫЕ С ОБРАБОТКОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

*Аннотация.* На сегодняшний день сотрудник является одним из важнейших ресурсов предприятия. Качество данного ресурса напрямую влияет на конкурентные преимущества, а также стратегические перспективы и возможности предприятия. В последнее время все чаще говорят о кадровой безопасности предприятия. Основой кадровой безопасности является в первую очередь подбор персонала, а также его оценка и аттестация. Подбор персонала — очень сложная задача, решением которой занимаются индивидуально в каждой компании, разрабатывая все новые и новые методики. Методик подбора персонала на сегодняшний день существует множество, но, несмотря на это, проблема кадров остается очень острой. Разработанная методика включает в себя тестирование, компетентностное и стрессовое интервью, решение кейсов, решение практических ситуаций, деловые игры.


© Глухарева С. В., 2017